(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 February 2004 (12.02.2004)

PCT

(10) International Publication Number
WO 2004/014037 A1

(51) International Patent Classification[7]: H04L 29/06, G06F 1/00

(21) International Application Number: PCT/IB2003/002932

(22) International Filing Date: 27 June 2003 (27.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02078076.3 26 July 2002 (26.07.2002) EP

(71) Applicant *(for all designated States except US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: KAMPERMAN, Franciscus, L., A., J. [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: GROENENDAAL, Antonius, W., M.; Philips Intellectual Property & Standards, Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

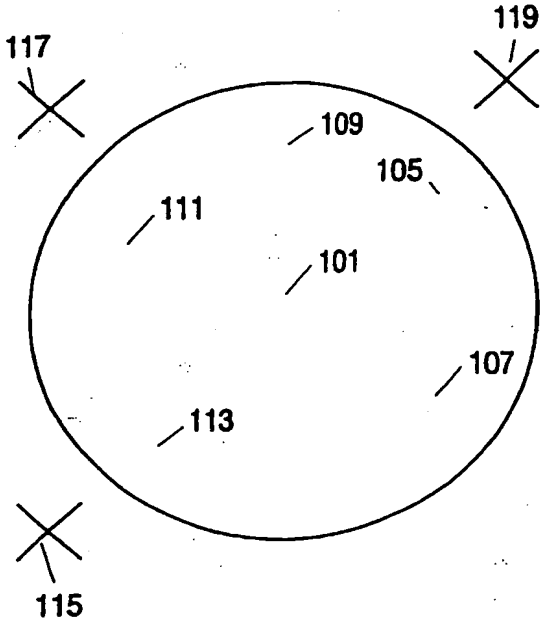
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR,*

[Continued on next page]

(54) Title: SECURE AUTHENTICATED DISTANCE MEASUREMENT



(57) Abstract: The invention relates to a method for a first communication device to performing authenticated distance measurement between said first communication device and a second communication device, wherein the first and the second communication device share a common secret and said common secret is used for performing the distance measurement between said first and said second communication device. The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device. Moreover, the invention relates to a communication device for performing authenticated distance measurement to a second communication device. The invention also relates to an apparatus for playing back multimedia content comprising a communication device.

WO 2004/014037 A1

Secure authenticated distance measurement

The invention relates to a method for a first communication device to performing authenticated distance measurement between a first communication device and a second communication device. The invention also relates to a method of determining whether data stored on a first communication device is to be accessed by a second communication device. Moreover, the invention relates to a communication device for performing authenticated distance measurement to a second communication device. The invention also relates to an apparatus for playing back multimedia content comprising a communication device.

Digital media have become popular carriers for various types of data information. Computer software and audio information, for instance, are widely available on optical compact disks (CDs) and recently also DVD has gained in distribution share. The CD and the DVD utilize a common standard for the digital recording of data, software, images, and audio. Additional media, such as recordable discs, solid-state memory, and the like, are making considerable gains in the software and data distribution market.

The substantially superior quality of the digital format as compared to the analog format renders the former substantially more prone to unauthorized copying and pirating, further a digital format is both easier and faster to copy. Copying of a digital data stream, whether compressed, uncompressed, encrypted or non-encrypted, typically does not lead to any appreciable loss of quality in the data. Digital copying thus is essentially unlimited in terms of multi-generation copying. Analog data with its signal to noise ratio loss with every sequential copy, on the other hand, is naturally limited in terms of multi-generation and mass copying.

The advent of the recent popularity in the digital format has also brought about a slew of copy protection and DRM systems and methods. These systems and methods use technologies such as encryption, watermarking and right descriptions (e.g. rules for accessing and copying data).

Because the common secret is being used for performing the distance measurement, it can be ensured that when measuring the distance from the first communication device to the second communication device, it is the distance between the right devices that is being measured.

The method combines a distance measurement protocol with an authentication protocol. This enables authenticated device compliancy testing and is efficient, because a secure channel is anyhow needed to enable secure communication between devices and a device can first be tested on compliancy before a distance measurement is executed.

In a specific embodiment, the authenticated distance measurement is performed according to the following steps,

- transmitting a first signal from the first communication device to the second communication device at a first time t1, said second communication device being adapted for receiving said first signal, generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal to the first device,
- receiving the second signal at a second time t2,
- checking if the second signal has been modified according to the common secret,
- determining the distance between the first and the second communication device according to a time difference between t1 and t2.

When measuring a distance by measuring the time difference between transmitting and receiving a signal and using a secret, shared between the first and the second communication device, for determining whether the returned signal really originated from the second communication device, the distance is measured in a secure authenticated way ensuring that the distance will not be measured to a third communication device (not knowing the secret). Using the shared secret for modifying the signal is a simple way to perform a secure authenticated distance measurement.

In a specific embodiment the first signal is a spread spectrum signal. Thereby a high resolution is obtained and it is possible to cope with bad transmission conditions (e.g. wireless environments with a lot of reflections).

In another embodiment the step of checking if the second signal has been modified according to the common secret is performed by the steps of,

- generating a third signal by modifying the first signal according to the common secret,
- comparing the third signal with the received second signal.

In a specific embodiment the data stored on the first device is sent to the second device if it is determined that the data stored on the first device are to be accessed by the second device.

The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of performing a distance measurement between a third communication device and the second communication device and checking whether said measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to the above. In this embodiment, the distance is not measured between the first communication device, on which the data are stored, and the second communication device. Instead, the distance is measured between a third communication device and the second communication device, where the third communication device could be personal to the owner of the content.

The invention also relates to a communication device for performing authenticated distance measurement to a second communication device, where the communication device shares a common secret with the second communication device and where the communication device comprises means for measuring the distance to the second device using said common secret.

In an embodiment the device comprises,

- means for transmitting a first signal to a second communication device at a first time t1, said second communication device being adapted for receiving said first signal, generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal,
- means for receiving the second signal at a second time t2,
- means for checking if the second signal has been modified according to the common secret,
- means for determining the distance between the first and the second communication device according to a time difference between t1 and t2.

The invention also relates to an apparatus for playing back multimedia content comprising a communication device according to the above.

In the following preferred embodiments of the invention will be described referring to the figures, wherein

second device 203 is a compliant device and might also comprise the step of checking whether the second device 203 really is the device identified to the first device 201. Then in 207, the first device 201 exchanges a secret with the second device 203, which e.g. could be performed by transmitting a random generated bit word to 203. The secret should be shared securely, e.g. according to some key management protocol as described in e.g. ISO 11770.

Then in 209, a signal for distance measurement is transmitted to the second device 203; the second device modifies the received signal according to the secret and retransmits the modified signal back to the first device. The first device 201 measures the round trip time between the signal leaving and the signal returning and checks if the returned signal was modified according to the exchanged secret. The modification of the returned signal according to some secret will most likely be dependent on the transmission system and the signal used for distance measurement, i.e. it will be specific for each communication system (such as 1394, Ethernet, Bluetooth, ieee 802.11, etc.).

The signal used for the distance measurement may be a normal data bit signal, but also special signals other than for data communication may be used. In an embodiment spread spectrum signals are used to be able to get high resolution and to be able to cope with bad transmission conditions (e.g. wireless environments with a lot of reflections).

In a specific example a direct sequence spread spectrum signal is used for distance measurement; this signal could be modified by XORing the chips (e.g. spreading code consisting of 127 chips) of the direct sequence code by the bits of the secret (e.g. secret consists also of 127 bits). Also, other mathematical operations as XOR could be used.

The authentication 205 and exchange of secret 207 could be performed using the protocols described in some known ISO standards ISO 9798 and ISO 11770. For example the first device 201 could authenticate the second device 203 according to the following communication scenario:

First device -> Second device: R_B||Text 1

where R_B is a random number

Second device -> First device: CertA||TokenAB

Where CertA is a certificate of A

TokenAB=R_A||R_B||B||Text3||sS_A(R_A||R_B||B||Text2)

signals are not identical, then the received signal cannot be authenticated and can therefore not be used for measuring the distance as illustrated by 325. In 323 the distance is calculated between the first and the second device; this could e.g. be performed by measuring the time, when the signal is transmitted by the transmitter 309 from the first device to the second device and measuring when the receiver 317 receives the signal from the second device. The time difference between transmittal time and receive time can then be used for determining the physical distance between the first device and the second device.

In figure 4 a communication device for performing authenticated distance measurement is illustrated. The device 401 comprises a receiver 403 and a transmitter 411. The device further comprises means for performing the steps described above, which could be by executing software using a microprocessor 413 connected to memory 417 via a communication bus. The communication device could then be placed inside devices such as a DVD, a computer, a CD, a CD recorder, a television and other devices for accessing protected content.

5. A method according to any of the claims 2, wherein the first signal and the common secret are bit words and where the second signal comprises information being generated by performing an XOR between the bit words.

6. A method according to any of the claims 1, wherein the common secret has been shared before performing the distance measurement, the sharing being performed by the steps of,

- performing an authentication check from the first communication device on the second communication device, by checking whether said second communication device is compliant with a set of predefined compliance rules,
- if the second communication device is compliant, sharing said common secret by transmitting said secret to the second communication device.

7. A method according to claim 6, wherein the authentication check further comprises checking if the identification of the second device is compliant with an expected identification.

8. A method of determining whether data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of performing a distance measurement between the first and the second communication device and checking whether said measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to claim 1.

9. A method according to claim 8, wherein the data stored on the first device are sent to the second device if it is determined that the data stored on the first device are to be accessed by the second device.

10. A method of determining whether data stored on a first communication device is to be accessed by a second communication device, the method comprising the step of performing a distance measurement between a third communication device and the second communication device and checking whether said measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to claim 1.

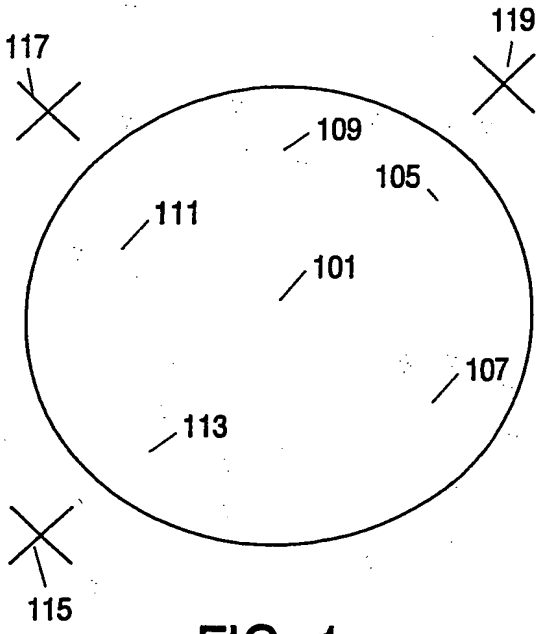

117
119
109
105
111
101
107
113
115

FIG. 1

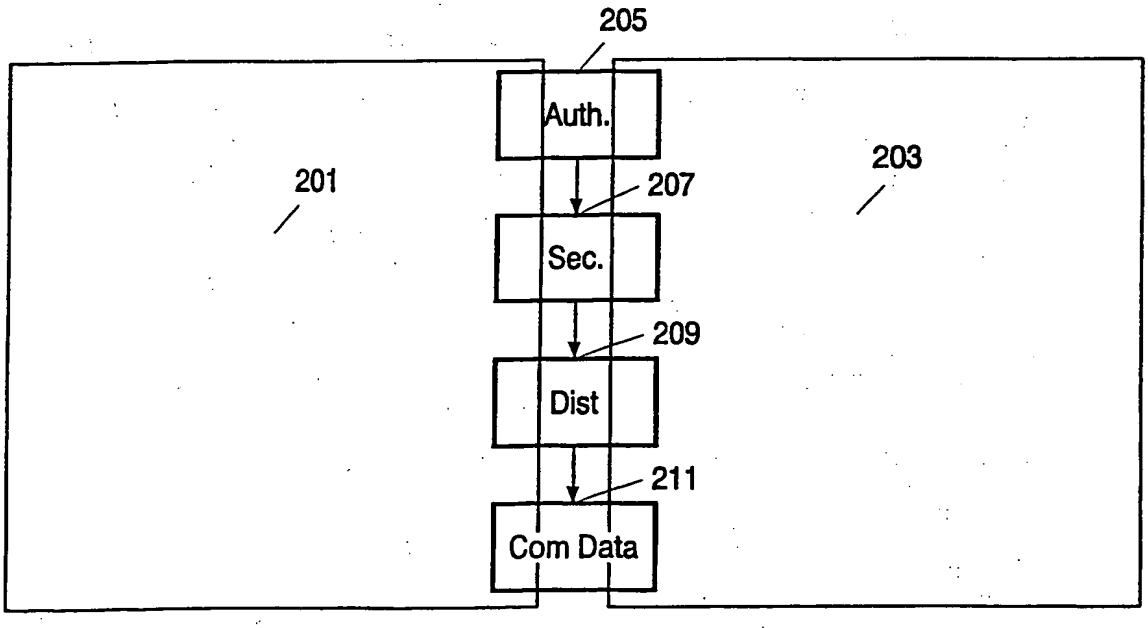

205
Auth.
201
203
207
Sec.
209
Dist
211
Com Data

FIG. 2

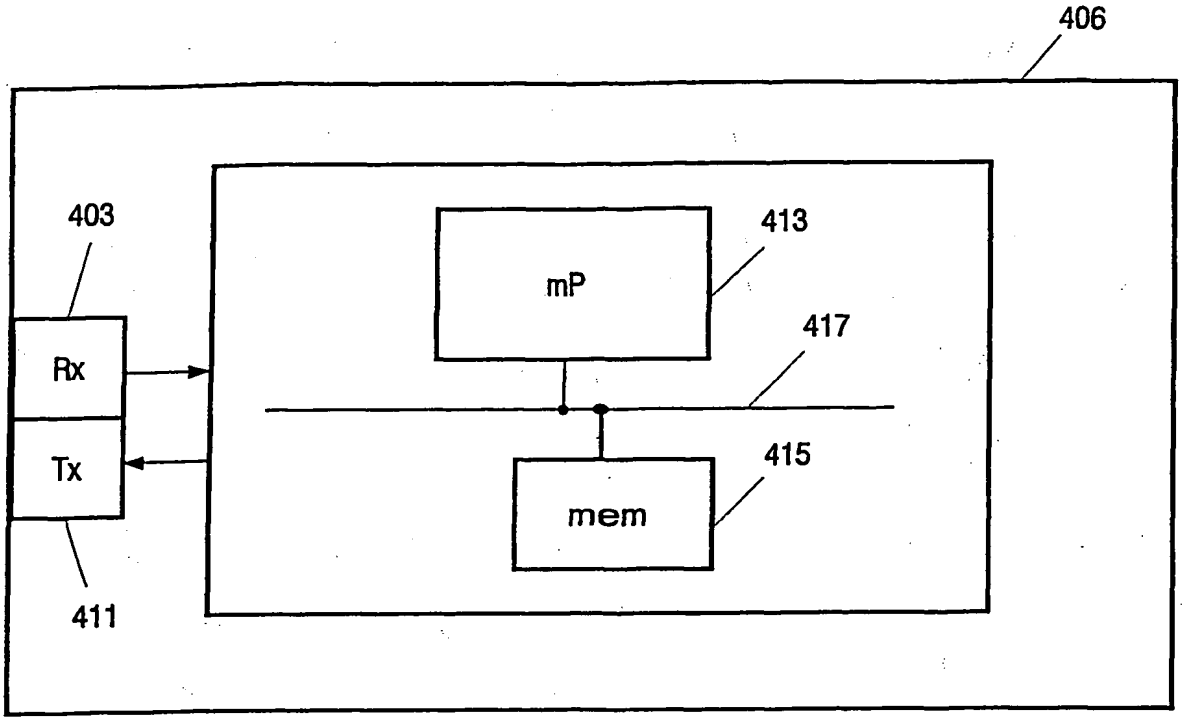


FIG. 4

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 97 39553 A (DAVIS DEREK L ;INTEL CORP (US); SMITH LIONEL (US)) 23 October 1997 (1997-10-23) page 4, line 2-19 page 7, line 20-26 page 11, line 8 -page 13, line 16 page 14, line 26 -page 15, line 6	1-13
P,X	US 2003/065918 A1 (WILLEY WILLIAM DANIEL) 3 April 2003 (2003-04-03) paragraph '0018! paragraphs '0070!-'0077! paragraph '0083!	1-13